TTPs used by DEV-0586 APT Group in WhisperGate Attack Targeting Ukraine

Huseyin Can YUCEEL & | January 17, 2022

On January 15, 2021, Microsoft Threat Intelligence Center (MSTIC) published a blog post stating that nation-state threat group DEV-0586 has been conducting destructive malware operations on Ukrainian organizations. In this blog, we share information about the simulation and mitigation of these malware attacks to help the cybersecurity community.

WhisperGate Wiper Malware

WhisperGate is a two-stage wiper malware that misrepresents itself as ransomware. The initial access stage for the malware is unknown at the moment. However, it is suspected to be a supply chain attack [1].

In its first stage, WhisperGate malware overwrites Master Boot Records (MBR) with a fake ransom note. Since the MBR is overwritten, it is not possible to recover it. Therefore, the ransom note is a misdirection, paying the ransom would not help recover lost data. After the first stage of the malware overwrites the MBR, powering down the infected system effectively bricks the system making it unable to boot up.

In its second stage, WhisperGate malware corrupts files with certain extensions and in certain directories by overwriting them with 0xCC bytes. After overwriting and corrupting files, the malware renames the files with a random four-byte extension.

Validate your Security Controls Against WhisperGate Malware Now

TTPs Used by DEV-0586 APT Group in WhisperGate Campaign

DEV-0586 hacking group uses the following tactics, techniques, and procedures (TTPs) in their WhisperGate wiper malware campaign:

Tactic: Execution

MITRE ATT&CK T1059.003 Command and Scripting Interpreter: Windows Command Shell

The first stage of WhisperGate malware uses the following Windows Command Shell command to execute the destructive malware:

```
cmd.exe /Q /c start c:\stage1.exe 1> \\127.0.0.1\ADMIN$\__[TIMESTAMP] 2>&1
```

MITRE ATT&CK T1059.001 Command and Scripting Interpreter: PowerShell

The second stage of WhisperGate malware uses PowerShell commands to connect its Command and Control (C2) server and download additional payloads [2].

```
powershell.exe -enc
UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==
```

The -enc parameter is used in this PowerShell command. However, there is not a parameter named -enc according to the official PowerShell documentation. In fact, the -enc parameter is completed by PowerShell as the -EncodedCommand parameter because of the parameter substring completion feature of PowerShell.

-EncodedCommand accepts a base-64-encoded string version of a command. Therefore, we must use base64 decoding to reveal the following PowerShell command:

```
Start-Sleep -s 10
```

Base64 Encoded	**Decoded**
UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==	Start-Sleep -s 10

Tactic: Defense Evasion & Persistence

MITRE ATT&CK T1542.003 Pre-OS Boot: Bootkit

The first stage of WhisperGate modifies the Master Boot Record (MBR). Since the altered MBR is the first section of the disk after completing hardware initialization by the BIOS, the malware evades defense.

MITRE ATT&CK T1027 Obfuscated Files or Information

The second stage of WhisperGate malware delivers PowerShell commands in Base64

Tactic: Discovery

MITRE ATT&CK T1083 File and Directory Discovery

The second stage of WhisperGate searches for specific file extensions in certain directories to alter their content.

Tactic: Command and Control

MITRE ATT&CK T1105 Ingress Tool Transfer

The second stage of WhisperGate download file corruptor payload from Discord channel hosted by the APT group. The download link for the malicious executable is hardcoded in the stage2.exe.

Tactic: Impact

MITRE ATT&CK T1561 Disk Wipe

The first stage of WhisperGate overwrites the Master Boot Record for impact. When the MBR is overwritten, the infected system does not boot up after power down.

The second stage of WhisperGate overwrites files and adversely affects their integrity. Also, the malware renames the files to further its impact.

WhisperGate Attack Simulations with Picus

Picus Continuous Security Validation Platform tests your security controls against WhisperGate malware variants and suggests related prevention methods.

Picus Labs advises you to simulate these malware families and determine the effectiveness of your security controls against them. Picus Threat Library consists of eight attack simulations for WhisperGate MBR Wiper malware of DEV-0586 APT group.

Threat Name
WhisperGate MBR Wiper Malware used by DEV-0586 Threat Group .EXE File Download (1 Variant
WhisperGate MBR Wiper Downloader used by DEV-0586 Threat Group .EXE File Download (2 Variants)
WhisperGate MBR Wiper Malware used by DEV-0586 Threat Group .DLL File Download (5 Variants)

Validate your Security Controls Against WhisperGate Malware

Indicators of Compromises

SHA-256	MD5	SHA-1
9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d	e61518ae9454a563b8f842286bbdb87b	82d29b52e35e7938e7ee610c04ea9daaf5e08e90
00bc665d96ecadc6beb2a9384773a70391f08f8e7a2876253f32ceec793eb728	ba45247858c0739865a52996768b7485	aff0b6eab23bbf4e5cb94fd4292c6d961dee060e
9cdaacaba35c3a473ec5b652d035a9593ee822609e79662223869e2b7298dc0a	ee47d6ae8414f6c6ca28a3b76bf75e44	a983bd69a71322d64199e67f2abcfe5ef0e1bca7
bbe1949ffd9188f5ad316c6f07ef4ec18ba00e375c0e6c2a6d348a2a0ab1e423	db600240aecf9c6d75c733de57f252bf	8756712e2c73ee3f92ded3852e41a486be3de6e2
ff3b45ecfbbdb780b48b4c829d2b6078d8f7673d823bedbd6321699770fa3f84	6f93fd91f17130aabd5251e7bae3eeaa	2af6e61d203191b4b8df982f37048937a1f9696c
35ab54a9502e975c996cbaee3d6a690da753b4af28808d3be2054f8a58e5c7c5	56af47c87029b9fba5fe7c81e99cedca	ea65565404ffde218ebccaeaca00ac1a2937dc57
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	14c8482f302b5e81e3fa1b18a509289d	16525cb2fd86dce842107eb1ba6174b23f188537
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	5d5c99a08a7d927346ca2dafa7973fc1	189166d382c73c242ba45889d57980548d4ba37e

References

[1] F. Bajak, “Microsoft discloses malware attack on Ukraine govt networks,” *Associated Press*, 16-Jan-2022. [Online]. Available: https://apnews.com/article/technology-business-europe-russia-ukraine-404c5e751709fba66b31fd512f734d80.

[2] Joe Security LLC, “Automated Malware Analysis Report for stage2.exe - Generated by Joe Sandbox,” Joe Security LLC. [Online]. Available: https://www.joesandbox.com/analysis/553986/0/html. [Accessed: 17-Jan-2022]

Share this:

DISCOVER
MORE RESOURCES

MITRE ATT&CK T1082 System Information Discovery

READ MORE →

Email*

□ I would like to receive emails including latest blog posts about emerging threats, events, product news, and more from Picus.*

Subscribe

United States

149 New Montgomery St 4th Floor
San Francisco, CA 94105
+1 (415) 890 5105

3001 North Rocky Point Drive East
Suite 200
Tampa, FL 33607 USA
+1 (336) 510 2907

United Kingdom

Work.Life Soho,
9 Noel Street, London, W1F 8GQ, UK
+44 20 38077425

Singapore

331 North Bridge Road,
Odeon Towers, #22-05 188720 Singapore
+65 3 1595424

Türkiye

Hacettepe Teknokent, Üniversiteler Mah.
1596. Cad. 1. Ar-Ge 97/12 Beytepe,
Çankaya/ Ankara, TR
+90 (312) 235 3579

Email

info@picussecurity.com

Platform

The Complete Security Validation Platform

Security Control Validation

Security Control Validation for Prevention Controls

Security Control Validation for Detection Controls

Attack Path Validation
Detection Rule Validation

Integrations

Network Security Technologies
Security Incident and Event Management (SIEM)
Endpoint Detection and Response (EDR)
Security Orchestration, Automation and Response (SOAR)

Use Cases

Security Posture Management
Security Control Validation
Security Control Rationalization
Enhancing Detection Efficacy
Compliance Enablement

Resources

Reports & Guides
Webinars
Newsletter
MITRE ATT&CK
Purple Academy

Partners

Technology Alliances
About the Partner Program
Become a Picus Partner

Company

About Us
Careers
Contact
Customer Support Portal
Trust Center